



CSEC-S

Introduction

FALL 2017

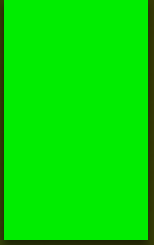
BY KC UDONSI

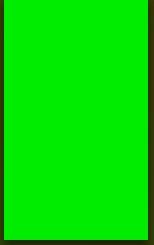
>\$ finger

- ▶ Udonsi Kc
- ▶ 5th year CS Specialist (Co-op)
- ▶ Specializing in Penetration testing, Exploitation, Malware Analysis and Digital forensics

>\$ help | less

- ▶ Computer Science Enrichment Club –
Computer and Network Security Division
- ▶ Fridays 3pm - 5pm
- ▶ Focus 1: Practical knowledge of Computer
and Network Security achieved by
understanding and solving Capture the
Flag challenges

- 
- ▶ Capture the flag challenges are typically grouped into the following:
 - ▶ PWN (Exploitation)
 - ▶ Web Applications & Network
 - ▶ Reverse Engineering
 - ▶ Cryptography
 - ▶ Forensics Analysis
 - ▶ Miscellaneous
 - ▶ Focus 2: General knowledge of Computer and Network Security

- 
- ▶ Computer Ethics
 - ▶ Secure Programming
 - ▶ Understanding the attack life-cycle
 - ▶ Understanding the vulnerability life cycle
 - ▶ *NIX OS secure practices
 - ▶ Windows OS secure practices
 - ▶ Required Text: Hacking; the art of exploitation 2nd Ed.
 - ▶ Amazon:
<https://www.amazon.ca/Hacking-Art-Exploitation-Jon-Erickson/dp/1593271441>

- ▶ Syllabus: security.csec.club/syllabus
- ▶ Resources:
 - ▶ Videos:
 - ▶ LiveOverflow YouTube channel
 - ▶ Open Security Training channel
 - ▶ Websites:
 - ▶ www.liveoverflow.com
 - ▶ www.opensecuritytraining.info/Training.html
 - ▶ Challenge sites:
 - ▶ www.exploit-exercises.com
 - ▶ www.overthewire.org
 - ▶ ctftime.org

BREAK!

Computer Ethics

- ▶ With great power comes great responsibility
- ▶ As Computer and Network Security professions (to be), it is important to understand the social implications of our actions
- ▶ Steven Levy described an acceptable list of ethics in his book 'Hackers: Heroes of the Computer Revolution'

Ethical and Legal Behavior

- ▶ During the course of the club, you may learn skills that will be considered illegal outside controlled environment
- ▶ The fact that you learn these skills does not permit use of said skills without consent or controlled environment
- ▶ The availability of a vulnerability does not imply it should be exploited.
- ▶ Taken from CSCD27 Ethical and Legal Behavior

Tools and installations required

- ▶ Windows OS users
 - ▶ Virtual box
 - ▶ Python 2.7
- ▶ MacOS users
 - ▶ Virtual box
- ▶ UNIX users
 - ▶ TBD

Meeting format

- ▶ First hour
 - ▶ Lesson hour. Any of:
 - ▶ Exploitation
 - ▶ Reverse Engineering
 - ▶ Cryptography
 - ▶ Web Application
 - ▶ Forensics

Meeting format Cont.

- ▶ Second hour
 - ▶ Challenge hour. Any of
 - ▶ Text book exercises
 - ▶ Watching and analyzing a solution video
 - ▶ Solving challenges from a challenge site
 - ▶ Reading and analyzing a solution write-up
 - ▶ Interactive session

Getting started

- ▶ Hacking: The art of Exploitation 2nd Ed.
 - ▶ Read Chapters 1 and 2
 - ▶ Ask questions on slack
 - ▶ The book CD is important. Helps to follow along the examples. You need it.
 - ▶ Don't stress if you don't understand. That's why I am here

Recap

- ▶ Get the book
- ▶ Signup
- ▶ Misuse of skills learned or shown is criminal and punishable under law
- ▶ The resources are there for you to work on your own
- ▶ Next week is reading week. No meeting.